

BLEICHMAR FONTI & AULD LLP

Lesley E. Weaver (SBN 191305)

555 12th Street, Suite 1600

Oakland, CA 94607

Tel.: (415) 445-4003

Fax: (415) 445-4020

lweaver@bfalaw.com

DiCELLO LEVITT GUTZLER LLC

Amy E. Keller, *pro hac vice to be filed*

Ten North Dearborn Street

Sixth Floor

Chicago, IL 60602

Tel.: (312) 214-7900

Fax: (440) 953-9138

akeller@dicellolevitt.com

Counsel for Plaintiffs and the Proposed Class

UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF CALIFORNIA
SAN JOSE DIVISION

APARNA IYER and BRANDY JOHNSON, *on*
behalf of themselves and all others similarly
situated,

Plaintiffs,

v.

TIKTOK INC., a California corporation, and
BYTEDANCE, INC., a Delaware corporation,

Defendants.

Case No.: 3:20-cv-03795

CLASS ACTION

CLASS ACTION COMPLAINT

DEMAND FOR JURY TRIAL

1 Plaintiffs Aparna Iyer and Brandy Johnson, individually and on behalf of all others similarly
2 situated, bring this class action against TikTok Inc. (“TikTok”), the successor-in-interest to Musical.ly,
3 Inc., and ByteDance, Inc. (“ByteDance”) (collectively, “Defendants”), and allege as follows based on
4 investigation of counsel, information, and belief:

5 **NATURE OF THE CASE**

6 1. Defendant TikTok maintains and operates a popular social media application (“TikTok
7 App” or “App”) that allows users to view, share, upload, and create short videos. Individuals who wish to
8 upload videos to the platform in addition to viewing posts from other users must download the App and
9 create an account.

10 2. Unknown and undisclosed to users, Defendants engage in a number of practices that violate
11 various state consumer protection and privacy laws—including obtaining and storing biometric and video
12 viewing information, not providing consumers with a retention schedule for use and storage of biometric
13 information, and tracking and disclosing user watch histories without appropriate consent

14 3. Defendants’ violations of state and federal laws are particularly egregious given previous
15 security and privacy complaints about Defendants’ mobile applications. Defendants continue to ignore
16 consumers’ legitimate privacy concerns even after paying millions in fines for their conduct, and continue
17 to engage in deceptive practices to ensure that consumers have little understanding about what types of
18 information they are sharing with the App and third parties.

19 4. This action seeks an order (i) enjoining Defendants’ from further unauthorized collection,
20 storage, and use of certain of Plaintiffs’ information; (ii) declaring that Defendants’ conduct violates the
21 Computer Fraud and Abuse Act, the Video Privacy Protection Act, the Illinois Biometric Information
22 Privacy Act, and certain sections of the California Penal Code; (iii) finding that Plaintiffs and the class
23 members are entitled to quantum meruit and damages for unjust enrichment based upon Defendants’
24 actions; (iv) invalidating Defendants’ use of mandatory, binding arbitration via inconspicuous terms to
25 prevent consumers from pursuing their rights under state and federal law; and (v) requiring Defendants to
26 clearly and conspicuously disclose its written policy that sets forth its retention and use of Plaintiffs’ and
27 class members’ biometric information.
28

PARTIES

Plaintiffs

5. Plaintiff Aparna Iyer (“Iyer”) is a citizen and resident of the State of California. Plaintiff created her TikTok account approximately nine months ago and maintains her account to the present day.

6. Plaintiff Iyer has uploaded and posted at least one video using TikTok, which includes images of her face and a friend’s face, since creating her account. Plaintiff Iyer has also appeared in friends’ videos, which have included the use of a combination of TikTok features such as stickers, filters, and the tracker lens available in the App when creating, saving, and posting videos on the App.

7. Plaintiff Iyer has also viewed and “liked” other videos, commented on videos, and sent messages to other viewers concerning their videos.

8. Plaintiff Iyer does not recall seeing the Terms of Service or Privacy Policy upon registering for an account with the App. Based on counsel’s investigation and analysis, set forth in detail below, TikTok deliberately designed its Terms of Service and Privacy Policy to decrease the likelihood that a user will notice and comprehend its terms and conditions or could provide meaningful, express consent to its conditions, in order to encourage users to sign up and not be deterred by accurate and truthful disclosures.

9. Plaintiff Brandy Johnson (“Johnson”) is a citizen and resident of the State of Illinois. Plaintiff created her TikTok account approximately six months ago and maintains her account to the present day.

10. Plaintiff Johnson has uploaded and posted at least one video using TikTok, which includes images of her face, since creating her account. Plaintiff Johnson has also used a combination of TikTok features such as stickers, filters, and the tracker lens available in the App when creating, saving, and posting videos on the App.

11. Plaintiff Johnson has also viewed and “liked” other videos, commented on videos, and sent messages to other viewers concerning their videos.

12. Plaintiff Johnson does not recall seeing the Terms of Service or Privacy Policy upon registering for an account with the App. Based on counsel’s investigation and analysis, set forth in detail

below, TikTok deliberately designed its Terms of Service and Privacy Policy to decrease the likelihood that a user will notice and comprehend its terms and conditions or could provide meaningful, express consent to its conditions, in order to encourage users to sign up and not be deterred by accurate and truthful disclosures.

Defendants¹

13. Defendant TikTok, Inc. is a California corporation with its headquarters in Culver City, California. Defendant TikTok maintains an office in Mountain View, California. Defendant TikTok is the surviving successor-in interest to Musical.ly, Inc. (“Musical.ly”). Musical.ly launched the Musical.ly Application (“Musical.ly App”) in 2014. In 2018, the Musical.ly App was rebranded as TikTok.

14. Defendant ByteDance, Inc. is a Delaware corporation with its headquarters in Palo Alto, California. Beijing ByteDance Technology Co. Ltd. (“ByteDance Ltd.”), a Beijing-based company founded in 2012, is the parent corporation of ByteDance, Inc.

15. DOE defendants. Plaintiffs reserve the right to name additional defendants, including Defendants’ corporate parents, based upon further analysis.

JURISDICTION AND VENUE

16. This Court has jurisdiction under the Class Action Fairness Act, 28 U.S.C. § 1332, because (i) this is a proposed class action in which there are at least 100 class members, (ii) the parties are minimally diverse, as Plaintiffs and Defendants are domiciled in different states, and (iii) the combined claims of class members exceed \$5,000,000, exclusive of interest, attorneys’ fees, and costs.

17. This Court has personal jurisdiction over Defendants because both Defendants regularly conduct business throughout California, their principal places of business are in California, and Defendant TikTok is incorporated in California.

18. Venue is proper in this District because a substantial part of the events or omissions giving rise to Plaintiffs’ claims occurred here, and Defendants caused harm to class members residing within this judicial District.

¹ Plaintiffs may add additional defendants—such as Beijing ByteDance Technology Co. Ltd., which is headquartered in Beijing, China—after additional discovery further demonstrates its connection to the allegations set forth herein.

INTRADISTRICT ASSIGNMENT

19. Pursuant to Civil Local Rule 3-2, this action may be assigned to the San Jose Division, as the events giving rise to the causes of action alleged herein occurred throughout the counties comprising this judicial District, including Santa Clara County.

COMMON FACTUAL ALLEGATIONS

A. Overview of the TikTok App and Its Predecessor Musical.ly

20. Musical.ly, Inc. and Musical.ly, a Cayman Island corporation, first created a social media video platform through a software application in 2014 (the “Musical.ly App”). Like the current version of the TikTok App, the Musical.ly App allowed users to create and edit short videos. It also provided a library of music that the user could apply as background music to their video, in effect allowing the user to create their very own music video. The Musical.ly App included several features that scanned the user’s facial geometry. These features included face stickers and face filters, which would alter the image of the user’s face.

21. While the Musical.ly App was growing in popularity in the U.S., ByteDance Ltd., the parent corporation to Defendant ByteDance, Inc., created the TikTok App in 2016. The App mirrored the purpose and features of the Musical.ly App, allowing users to create and upload videos.

22. In 2017, ByteDance, Inc., acquired Musical.ly, for \$1 billion, and rebranded Musical.ly to TikTok, Inc.

23. On August 2, 2018, TikTok merged the Musical.ly and TikTok Apps. Following its merger, the TikTok App has continued expanding its user base. As of November 2019, the TikTok App has over 26.5 million U.S. users and was the most downloaded application on the Apple app store.²

24. The App is predominantly used by young adults and minors. Indeed, at least two-thirds of U.S. users are teenagers or in their twenties.³

² Ansoor Iqbal, *TikTok Revenue and Usage Statistics (2020)*, Business of Apps (Apr. 24, 2020), <https://www.businessofapps.com/data/tik-tok-statistics/>.

³ Greg Roumeliotis, et al., *Exclusive: U.S. opens national security investigation into TikTok – sources*, Reuters (Nov. 1, 2019), <https://www.reuters.com/article/us-tiktok-cfius-exclusive/exclusive-u-s-opens-national-security-investigation-into-tiktok-sources-idUSKBN1XB4IL>.

25. TikTok’s popularity with younger users is by design. The TikTok algorithmic feed launches a never-ending-stream of videos at a user.⁴ The algorithm is constantly learning what content to deliver to its users to keep them engaged. A user receives videos based on those the user has already watched and interacted with.⁵ Users are encouraged to engage with other videos by responding in turn.

26. TikTok’s algorithms allow the App to mine extensive data regarding how its users react to videos—which, in turn, allows Defendants to understand how people think, feel, and act, “making [TikTok] an expert on what makes people tick and how to persuade them to watch, share [,] or like certain content.”⁶

27. TikTok did not disclose and still has not publicly revealed the ways in which it collects, monitors, surveils, and shares users’ activity on the platform as well as other information about users with unauthorized third parties. Plaintiffs would not have signed up on the platform if the true extent to which their biometric and other information was permanently copied and shared with third parties was revealed.

28. Given the nature of the App, and the extensive information it gathers on individuals, and predictions concerning individuals’ actions the App can make, U.S. lawmakers have labeled TikTok to be a “potential counterintelligence threat we cannot ignore.”⁷

B. Defendants Have an Established Record of Invading Users’ Privacy

29. Defendants have repeatedly disregarded users’ privacy by collecting, sharing, and using users’ information without obtaining consent.

30. In 2019, the Federal Trade Commission (“FTC”) filed a complaint against TikTok over allegations that it violated the Children’s Online Privacy Protection Act (“COPPA”), 15 U.S.C. §§ 6501,

⁴ John Herrman, *TikTok Is Rewriting the World*, N.Y. Times (Mar. 10, 2019), <https://www.nytimes.com/2019/03/10/style/what-is-tik-tok.html>.

⁵ Morgan Sung, *A Guide to using TikTok’s algorithm to watch videos you actually like*, Mashable (Jan. 13, 2020), <https://mashable.com/article/tiktok-algorithm-watch-what-you-actually-like/>.

⁶ Shelly Banjo, *Take China’s TikTok App Security Threat Seriously*, Bloomberg (Oct. 29, 2019), <https://www.bloomberg.com/news/newsletters/2019-10-29/worries-that-tiktok-is-a-threat-to-national-security-have-merit>.

⁷ *Id.*

1 *et seq.* Defendant TikTok settled the claim for \$5.7 million—at that time, the largest penalty ever imposed
2 for violation of COPPA.⁸

3 31. In November 2019, the United States government announced a national security review of
4 TikTok’s parent, ByteDance Ltd.’s acquisition of the Musical.ly app for \$1 billion.⁹ TikTok has been
5 banned by use for the United States Armed Forces, Department of Homeland Security, and the
6 Transportation Security Administration.¹⁰ The Department of Defense has determined that TikTok “is
7 considered a cyber threat” and as of December 2019, the Army and Navy no longer allow the App to be
8 installed on government-issued phones and devices.¹¹ Subsequently, the Air Force, Coast Guard, Marine
9 Corps, and Department of Homeland Security, and Transportation Security Administration issued the
10 same restrictions for their personnel.¹²

11 32. TikTok is considered such a high-level threat by the government, that Army public affairs
12 officer Crystal X. Boring stated:

- 13 • “The message directs appropriate action for employees to take in order to safeguard their
14 personal information. The guidance is to be wary of applications you download, monitor
15
16

17
18 ⁸ Lesley Fair, *Largest FTC COPPA settlement requires Musical.ly to change its tune*, FTC (Feb. 27,
19 2019), <https://www.ftc.gov/news-events/blogs/business-blog/2019/02/largest-ftc-coppa-settlement-requires-musically-change-its>.

20 ⁹ Jack Nicas, Mike Isaac, and Ana Swanson, *TikTok Said to Be Under National Security Review*, N.Y.
21 Times (Nov. 1, 2019), <https://www.nytimes.com/2019/11/01/technology/tiktok-national-security-review.html>.

22 ¹⁰ Mary Meisenzahl, *US government agencies are banning TikTok, the social media app teens are*
23 *obsessed with, over cybersecurity fears—here’s the full list*, Business Insider (Feb. 25, 2020),
<https://www.businessinsider.com/us-government-agencies-have-banned-tiktok-app-2020-2#7-this-week-tsa-became-the-latest-agency-to-specifically-ban-the-app-7>.

24 ¹¹ Matthew Cox, *Army Follows Pentagon Guidance, Bans Chinese-Owned TikTok App*, Military News
25 (Dec. 30, 2019), <https://www.military.com/daily-news/2019/12/30/army-follows-pentagon-guidance-bans-chinese-owned-tiktok-app.html>.

26 ¹² Mary Meisenzahl, *US government agencies are banning TikTok, the social media app teens are*
27 *obsessed with, over cybersecurity fears—here’s the full list*, Business Insider (Feb. 25, 2020),
28 <https://www.businessinsider.com/us-government-agencies-have-banned-tiktok-app-2020-2#5-the-marine-corps-expressed-similar-reasoning-for-a-ba%25E2%2580%25A6>.

your phones for unusual and unsolicited texts etc. and delete them immediately and uninstall TikTok to circumvent any exposure of personal information.”¹³

33. This guidance stemmed from scrutiny for ByteDance, TikTok’s owner, when Senators Chuck Schumer and Tom Cotton requested Joseph Maguire, the acting director of national intelligence, review TikTok for potential security risks.¹⁴ On information and belief, TikTok has in the past and/or presently continues a practice of removing content at the request of ByteDance, Inc. and other corporate entities.¹⁵

34. As Senators Schumer and Cotton wrote in their October 23, 2019 letter to Director Maguire concerning TikTok, “[s]ecurity experts have voiced concerns that China’s vague patchwork of intelligence, national security, and cybersecurity laws compel Chinese companies to support and cooperate with intelligence work controlled by the Chinese Communist Party. Without an independent judiciary to review requests made by the Chinese government for data or other actions, there is no legal mechanism for Chinese companies to appeal if they disagree with a request.”¹⁶

35. Senator Josh Hawley recently stated that, “[t]he idea that TikTok is not sharing any data, is not taking direction from Beijing, that just does not appear to be true.”¹⁷ Further, Senator Marsha Blackburn asserted: “TikTok is China’s best detective—surreptitiously collecting and sharing user data,

¹³ Kahlan Rosenblatt, *Army bans TikTok following guidance from the Pentagon*, NBC News (Dec. 31, 2019), <https://www.nbcnews.com/tech/tech-news/u-s-army-bans-tiktok-following-guidance-pentagon-n1109001>.

¹⁴ *Id.* Indeed, additional security risks have plagued the application—including code that would have allowed hackers to carry out malicious attacks. Arjun Kharpal, *A security flaw in China’s TikTok app was found. It lets hackers use text messages to control accounts*, CNBC (Jan. 9, 2020), <https://www.cnbc.com/2020/01/09/tiktok-security-flaw-found-that-allowed-hackers-to-access-accounts.html>.

¹⁵ Justine Calma, *US Army bans soldiers from using TikTok*, The Verge (Dec. 31, 2019), <https://www.theverge.com/2019/12/31/21044559/us-army-bans-soldiers-from-using-tiktok>.

¹⁶ Ben Kochman, *Sens. Want TikTok Investigated for National Security Threats*, Law360 (Oct. 24, 2019), <https://www.law360.com/articles/1213180/sens-want-tiktok-investigated-for-national-security-threats>.

¹⁷ Emily Birnbaum, *TikTok faces lawmaker anger over China ties*, The Hill (Nov. 5, 2019), <https://thehill.com/policy/technology/469114-tiktok-faces-lawmaker-anger-over-china-ties>.

1 tracking American tweens and teenagers, and manipulating children's online purchases."¹⁸ U.S. officials
 2 have expressed concerns about other social media apps China is developing itself as well.¹⁹

3 36. National legislation is currently being proposed that would ban all federal employees from
 4 using the App.²⁰

5 37. International investigations are also ongoing into TikTok's practices, which all seek to
 6 prevent the abuse of data collection and potential for national security risks.

7 38. Just recently, a Dutch privacy watchdog has announced that it will conduct an investigation
 8 of the TikTok App to determine whether the information provided to children "adequately explains how
 9 their personal data is collected, processed and used."²¹

10 39. In July 2019, the United Kingdom's Information Commissioner's Office's representative
 11 Elizabeth Denham stated, "We are looking at the transparency tools for children . . . We're looking at the
 12 messaging system, which is completely open, we're looking at the kind of videos that are collected and
 13 shared by children online. We do have an active investigation into TikTok right now, so watch this
 14 space."²² The investigation is ongoing.²³

18 ¹⁸ *Id.*

19 ¹⁹ Georgia Wells & Kate O'Keeffe, *U.S. Orders Chinese Firm to Sell Dating App Grindr Over*
 20 *Blackmail Risk*, The Wall Street Journal (March 27, 2019), <https://www.wsj.com/articles/u-s-orders-chinese-company-to-sell-grindr-app-11553717942>.

21 ²⁰ Alexandra S. Levine, *Senate bill would ban TikTok on federal employees' work phones*, Politico (Mar.
 22 12, 2020), <https://www.politico.com/news/2020/03/12/senate-bill-would-ban-tiktok-on-federal-employees-work-phones-126727>.

23 ²¹ Stephani Bodoni, *TikTok Faces Dutch Privacy Probe Over Children's Data*, Bloomberg Quint (May
 24 8, 2020), <https://www.bloombergquint.com/onweb/tiktok-faces-dutch-privacy-probe-over-safety-of-children-s-data>.

25 ²² Alex Hern, *TikTok under investigation over child data use*, The Guardian (Jul. 2, 2019),
 26 <https://www.theguardian.com/technology/2019/jul/02/tiktok-under-investigation-over-child-data-use>.

27 ²³ Press Association, *UK data regulator hones in on TikTok as it makes child safety top priority for 2020*
 28 (Dec. 26, 2019), <https://www.breakingnews.ie/world/uk-data-regulator-hones-in-on-tiktok-as-it-makes-child-safety-top-priority-for-2020-972258.html>.

40. The Italian Data Privacy Authority (DPA) launched a review of TikTok's collection and handling of users' data and called on the European Data Protection Board (EDPB) to set up an ad hoc task force regarding the same.²⁴

41. Investigations and bans by regulators exemplify the extreme disregard Defendants have shown for the privacy and security of its users.

C. TikTok Automatically Transfers Users' Personally Identifiable Information to Corporate Affiliates Around the World

42. Unbeknownst to users, TikTok is transferring users' personally identifiable video viewing information to TikTok's corporate affiliate. TikTok transfers this information to ByteDance Ltd. through at least three domains: maliva-mcs.byteoversea.com, sgali-mcs.byteoversea.com and monva.byteoversea.com. Upon information and belief, these domains are owned and operated by ByteDance Ltd. and are hosted in China.

43. TikTok transfers to ByteDance Ltd. information on videos viewed by the user as well as several unique identifying numbers ("Unique Identifiers") associated with the user. TikTok assigns each user a user identification number ("UID"). TikTok transmits this UID to ByteDance along with other personal information while a user is logged on to the platform. When a user visits her profile page, TikTok pairs the UID and other Unique Identifiers with the user's account name, profile page, and any additional information contained on the profile pages, such as a written biography or videos viewed by the user on her profile. In this way, ByteDance Ltd. can easily associate Unique Identifiers with the individual user.

44. For example, if a user has "liked" a video shared by the account of @Jasonderulo, she can view it from her profile page. When the user views this video, TikTok transmits the following information to the domain of either maliva-mcs.byteoversea.com or sgali-mcs.byteoversea.com:

- a. UID (e.g. 682319*****), a unique UID, a Service Set Identifier or (SSID) associated with the user's WiFi network, and a web_ID;
- b. The user's account name, which is included in the page_url (e.g. https://www.tiktok.com/@bob*****);

²⁴ Dario Betti, *TikTok under review by European Privacy authorities* (Jan. 29, 2020), <https://mobileecosystemforum.com/2020/01/29/tik-tok-under-review-by-european-privacy-authorities/>.

- c. The time the user watched the video (e.g. “Thu Jun 04 2020 10:52:19 GMT-0700 (Pacific Daylight Time)”);
- d. The overall duration of the video (e.g. “15.115”);
- e. The “play_duration,” which indicates how long the video was viewed (e.g. 4.3269244); and
- f. The precise URL of the video.²⁵

45. The information transmitted to these two domains also includes the region where the user resides by country (e.g. U.S.), time-zone of the user and the user’s device information.

46. TikTok associates the same UID to an individual user when it shares information to ByteDance Ltd. When a user logs on to TikTok from a new device, TikTok then begins associating the same UID to that user. Even after a user has cleared her browser history and cleared her cookies, TikTok will continue pairing the same UID with the video viewing information it transmits to ByteDance while the user is logged on. The additional Unique Identifiers that TikTok transmits allow ByteDance to continue identifying user’s viewing activity even when the user is no longer logged on but is still viewing videos on the platform.

47. As the user navigates through videos on TikTok’s platform, TikTok continues to transfer user’s personally identifying video viewing history. For example, if the user then watches a video hosted on the content creator page @johnlegendofficial, TikTok transmits the following information to either maliva-mcs.byteoversea.com or sgali-mcs.byteoversea.com:

- a. The same User Identifiers associated with that user including the UID (e.g. 682319*****”), unique UID, SSID, and web_id;
- b. The time the user watched the video (e.g. “Thu Jun 04 2020 10:52:19 GMT-0700 (Pacific Daylight Time)”);

²⁵ For purposes of illustrating this example, e.g. [https://v19.tiktokcdn.com/d750332c6ea1a13ae7fd03d218dc3b8a/5ed98954/video/tos/useast2a/tos-useast2a-ve-0068c001/8c33500946d64b6a87c21c8ce8f74ae7/?a=1233&br=3430&bt=1715&cr=0&cs=0&dr=0&ds=3&er=&l=20200604175237010189195216022B7F7F&lr=tiktok_m&mime_type=video_mp4&q=0&rc=amU7d3V5eWhndDMzaDczM0ApZjc0Ojo2OTs5N2gzO2Q6O2duZ3NhMV8wcmxflS0vMTZzc2M0Li81NWAzM18xXi8zM146Yw%3D%3D&vl=&vr=\",\"event_index\":1591293671691.](https://v19.tiktokcdn.com/d750332c6ea1a13ae7fd03d218dc3b8a/5ed98954/video/tos/useast2a/tos-useast2a-ve-0068c001/8c33500946d64b6a87c21c8ce8f74ae7/?a=1233&br=3430&bt=1715&cr=0&cs=0&dr=0&ds=3&er=&l=20200604175237010189195216022B7F7F&lr=tiktok_m&mime_type=video_mp4&q=0&rc=amU7d3V5eWhndDMzaDczM0ApZjc0Ojo2OTs5N2gzO2Q6O2duZ3NhMV8wcmxflS0vMTZzc2M0Li81NWAzM18xXi8zM146Yw%3D%3D&vl=&vr=\)

- c. The overall duration of the video (e.g. “27.236”);
- d. The “play_duration,” which indicates how long the video was viewed (e.g. 8.7599897); and
- e. The precise URL for the video.²⁶

48. Because TikTok pairs UIDs and other User Identifiers with additional information showing users’ video viewing history, users’ video viewing history are readily identifiable. TikTok continues to transmit personally identifiable video viewing history even after a user has logged out of her account.

49. Likewise, TikTok transmits video viewing information to mon-va.byteoversea.com that is paired with a unique identifier titled SLARDAR_WEB_ID. For example, if a user visits the page of content creator @willsmith and watches a video, TikTok transmits:

- a. The specific URL of the video
(e.g. <https://www.tiktok.com/@willsmith/video/6820541348022652166?lang=US>);
- b. The SLARDAR_WEB_ID of the user (e.g. c3754625-0ed7-468d-9d98-910e7a*****).

50. When a user visits her home page, the SLARDAR_WEB_ID can be easily associated with a user’s profile name because TikTok transfers the User’s homepage URL which includes the user name along with the SLARDAR_WEB_ID. A screenshot example of a portion of what TikTok transmits to mon-va.byteoversea.com is shown below:

²⁶ For purposes of demonstrating this example, e.g., [https://v16m.tiktokcdn.com/3ebf23bd9093f580fbea179aa6777fae/5ed995fb/video/tos/useast2a/tos-useast2a-ve-0068c002/77397da4922848edb50deb52565453c8/?a=1233&br=3438&bt=1719&cr=0&cs=0&dr=0&ds=3&er=&l=202006041846240101890660473735C389&lr=tiktok_m&mime_type=video_mp4&qs=0&r=c=MztnNzQ8a2pqdTMzaDczM0ApNDxpZjxmZsszN2hkNzg6ZWcvY3EvXmluNTZfLS1jMTZzcyc5fMS00Ly4uMF8zNDEvY2A6Yw%3D%3D&vl=&vr=", "event_index":1591295427844](https://v16m.tiktokcdn.com/3ebf23bd9093f580fbea179aa6777fae/5ed995fb/video/tos/useast2a/tos-useast2a-ve-0068c002/77397da4922848edb50deb52565453c8/?a=1233&br=3438&bt=1719&cr=0&cs=0&dr=0&ds=3&er=&l=202006041846240101890660473735C389&lr=tiktok_m&mime_type=video_mp4&qs=0&r=c=MztnNzQ8a2pqdTMzaDczM0ApNDxpZjxmZsszN2hkNzg6ZWcvY3EvXmluNTZfLS1jMTZzcyc5fMS00Ly4uMF8zNDEvY2A6Yw%3D%3D&vl=&vr=).

```

pid=others_homepage
protocol=https
report_domain=mon-v.a.byteoversea.com
report_type=xhr
reportURLSingle=https://mon-v.a.byteoversea.com/log/sentry/v2/api/slardar/main/
sample_rate=1
screen_resolution=1670x939
slardar_session_id=48446f0f-f51c-4f09-a43b-66db147a9848
slardar_web_id=c3754625-0ed7-468d-9d98-910e7a51fc99
url=https://www.tiktok.com/@boboboblaw?lang=en
version=3.4.11

```

51. TikTok continues to transfer video viewing history associated with the SLARDAR_WEB_ID to ByteDance Ltd., even after a user has logged off of her account.

D. TikTok's Targeted Advertising Practices

52. TikTok currently allows for targeted advertising based on age, gender, location, operating system, and network on the device.²⁷

53. Additionally, TikTok targets advertisements based users' interests and video viewing preferences, such as beauty, fashion, and food.²⁸ Though the feature has not yet been released in the U.S., TikTok has already released a native audience network in China and Japan, which will allow advertisers to place TikTok ads based on each user's video viewing preferences on a network of apps across devices.²⁹

54. TikTok also allows advertisers to coordinate pairing users' contact data, website traffic, app activity, or ad engagement with other TikTok data in order to create custom target audiences for advertising.³⁰

55. TikTok also continuously transmits to and exchanges information with companies such as Facebook and AppsFlyer about users' video views, subscribed channels, and search terms entered on

²⁷ *Ad Targeting*, TikTok Ads, <https://ads.tiktok.com/help/article?aid=6721969269619294213> (Last accessed June 5, 2020).

²⁸ *Interest Targeting*, TikTok Ads, <https://ads.tiktok.com/help/article?aid=6730493704647213061> (Last accessed June 5, 2020).

²⁹ Shubham Agarwal, *Get ready for targeted ads based on your TikTok watch history* (Aug. 27, 2019), <https://www.digitaltrends.com/social-media/tiktok-advertiser-audience-network-targeted-ads/>.

³⁰ Kristi Hines, *The Complete Guide to TikTok Advertising for Marketers* (March 16, 2020), <https://blog.hootsuite.com/tiktok-advertising/>.

1 TikTok.³¹ The information received from Facebook contains an advertising ID that can be assigned to a
 2 Facebook user when the user is logged into her Facebook account.³²

3 56. The advertising practices show no sign of slowing down and, in fact, TikTok has stated the
 4 opposite is true, promising more “interest, behavioral, and more granular [demographic] targeting over
 5 time.”³³

6 **E. TikTok’s Unlawful Use of Biometric Identifiers and Information**

7 57. The Illinois Biometric Privacy Information Act was enacted in 2008 to regulate the
 8 collection and use of biometrics. The statute recognizes that biometrics “unlike other unique identifiers”
 9 cannot be changed when compromised.³⁴

10 58. Under the BIPA, biometric identifiers means “retina or iris scan, fingerprint, voiceprint, or
 11 scan of hand or face geometry” and biometric information means “any information, regardless of how it
 12 is captured, converted, stored, or shared, based on an individual’s biometric identifier used to identify an
 13 individual.”³⁵

14 59. The statute further provides that:³⁶

15 (b) No private entity may collect, capture, purchase, receive through trade, or
 16 otherwise obtain a person’s or a customer’s biometric identifier or biometric
 17 information unless it first:

18 (1) informs the subject or the subject’s legally authorized representative in
 19 writing that a biometric identifier or biometric information is being
 20 collected or stored;

21
 22
 23 ³¹ Matthias Eberl, *How TikTok monitors its users*, Süddeutsche Zeitung (Dec. 4, 2019),
<https://www.sueddeutsche.de/digital/tiktok-ueberwachung-daten-kritik-1.4709779> (Google Translation).

24 ³² *Id.*

25 ³³ Mikey Dunn, *What You Need to Know About Advertising on TikTok* (Aug. 20, 2019),
<https://www.socialmediatoday.com/news/what-you-need-to-know-about-advertising-on-tiktok/561235/>.

26 ³⁴ 740 ILCS 14/5(c).

27 ³⁵ *Id.*

28 ³⁶ 740 ILCS 14/15.

(2) informs the subject or the subject's legally authorized representative in writing of the specific purpose and length of term for which a biometric identifier or biometric information is being collected, stored, and used; and (3) receives a written release executed by the subject of the biometric identifier or biometric information or the subject's legally authorized representative. . . .

60. Additionally, the statute provides that:³⁷

[A] private entity in possession of biometric identifiers or biometric information must develop a written policy, made available to the public, establishing a retention schedule and guidelines for permanently destroying biometric identifiers and biometric information when the initial purpose for collecting or obtaining such identifiers or information has been satisfied or within 3 years of the individual's last interaction with the private entity, whichever occurs first.

61. When a user creates a video on the TikTok App, the user can choose to apply effects that will apply a graphic animation onto the face of the user or that will alter the facial features of the user. TikTok categorizes these effects in groups labeled "Beauty," "Trending," and "Funny," to encourage users to access them. Users also have the option to use a face tracking lens that will detect and automatically zoom in on a user's face.

62. The Musical.ly App operated similar to the current version of the TikTok App, and also scanned, collected, and stored a user's facial geometry when that user applied a facial graphic feature, such as a sticker or facial filter.

63. One form of marketing offered by TikTok also includes "branded lenses," similar to the face filters already offered by TikTok, but allowing companies to provide their own filters.³⁸

³⁷ 740 ILCS 14/15(a).

³⁸ Mikey Dunn, *What You Need to Know About Advertising on TikTok*, Social Media Today (Aug. 20, 2019), <https://www.socialmediatoday.com/news/what-you-need-to-know-about-advertising-on-tiktok/561235/>.

64. Unbeknownst to the user, when a user engages in these features, TikTok collects, stores and maintains a copy of the user's facial geometry as well as biometric information derived from this copy. TikTok does not disclose to users that this information is being collected and stored, and it does not disclose how, or for how long, it is maintained.

65. Based upon preliminary expert analysis, the code is written in a specific way in order to extract facial landmarks and identify users' faces in images, specifically to identify where the face is, transform the representation of the face to an internal representation—to make geometry manipulation easier—and then convert it back to the pixels that are shown to users.

66. Upon information and belief, TikTok transfers copies of the users' facial geometry and derivative information to other corporate entities including Defendant ByteDance, Inc.

67. Preliminary expert analysis indicates that the video search functionality of the TikTok app would be severely diminished if TikTok was not storing biometric data as alleged herein. Web analysts have discovered that TikTok appears to harvest biometric data in order to create a search function—allowing users to search TikTok videos based upon the individuals who appear in them. And the App's use of face scanning allows users to “decorat[e] or distort[] their faces, all easily edited into a clip for other users to ‘like,’ ‘share’ or comment on.”³⁹ Based upon counsel's investigation, such search functions could not be efficiently performed if the data were not cached. That is, a search would otherwise take days.⁴⁰

68. Preliminary expert analysis also suggests TikTok may analyze users' faces even when they do not post videos and only post a profile picture.⁴¹ For example, TikTok provides content recommendations based upon TikTok users' physical appearance: an artificial intelligence researcher at University of California Berkeley School of Information “found that TikTok was recommending him

³⁹ Nick Frisch, *We Should Worry About How China Uses Apps Like TikTok*, NY Times (May 2, 2019), <https://www.nytimes.com/interactive/2019/05/02/opinion/will-china-export-its-illiberal-innovation.html>.

⁴⁰ Shubham Agarwal, *TikTok's creepy new feature lets you search for videos based on people's faces*, Digital Trends (Sept. 25, 2019), <https://www.digitaltrends.com/social-media/tiktok-facial-recognition-video-face-search-feature-china/>.

⁴¹ Marc Faddoul via Twitter: “A TikTok novelty: FACE-BASED FILTER BUBBLES,” <https://twitter.com/MarcFaddoul/status/1232014908536938498> (Last visited June 5, 2020).

1 accounts with profile pictures that matched the same race, age or facial characteristics as the ones he
2 already followed.”⁴²

3 69. Additional concerns regarding the links between the American and Chinese version of
4 TikTok—and in particular censorship, surveillance, and the use of facial recognition software—have also
5 raised alarms for consumer advocacy groups.⁴³

6 70. TikTok’s heavy reliance on artificial intelligence and machine learning has also set off
7 alarms with consumer advocacy groups, especially that the Chinese version of TikTok allows its users to
8 perform facial recognition on faces selected by users from other users’ videos.⁴⁴

9 71. TikTok makes no effort to disclose to users how their biometric information is used or
10 stored prior to their using the App.

11 **F. TikTok’s Collection and Disclosure of Users’ Watch History**

12 72. Upon launching the App, a user will see a page of videos that TikTok labels “For You.”
13 This is a customized collection of videos that Defendants have curated that they believe will meet a user’s
14 taste and interest the user based upon the users “likes” of prior videos. The vast bulk of those videos are
15 likely from people the user does not know, collated by the App’s algorithm.⁴⁵

16 73. TikTok’s algorithm is designed to ensure that users see videos and content that they like.
17 This algorithm also allows advertisers to design and optimize ad campaigns to users that are more likely
18 to click on them.⁴⁶

19
20
21 ⁴² Maria Mellor, *Why is TikTok creating filter bubbles based on your race?*, Wired (Feb. 28, 2020),
<https://www.wired.co.uk/article/tiktok-filter-bubbles>.

22 ⁴³ *Id.*; *TikTok: Should we trust the Chinese social-media video app?*, BBC News (Nov. 7, 2019),
<https://www.bbc.com/news/technology-50319690>.

23 ⁴⁴ Dan Robitzki, *TikTok Tracks Users With Facial Recognition*, Futurism.com (Sept. 19, 2019),
24 <https://futurism.com/the-byte/tiktok-facial-recognition>; Adan Kohnhorst, *TikTok’s New “Video Search”*
25 *Function is From the Future*, Raddi (Sept. 26, 2019), [https://radiichina.com/tiktok-new-video-search-](https://radiichina.com/tiktok-new-video-search-function-is-from-the-future/)
[function-is-from-the-future/](https://radiichina.com/tiktok-new-video-search-function-is-from-the-future/).

26 ⁴⁵ *How to Feature on TikTok’s “For You” Page*, Influencer Marketing Hub (Apr. 16, 2020),
<https://influencermarketinghub.com/tiktok-for-you-page/>.

27 ⁴⁶ *How Does Advertising on TikTok Work?*, Influencer Marketing Hub (Jan. 3, 2020),
28 <https://influencermarketinghub.com/advertising-on-tiktok/>.

74. Although TikTok only currently allows demographic targeting, the company may engage in interest, behavioral, and more granular demo marketing over time.⁴⁷

75. While TikTok innocuously claims that its data collection for advertising purposes allows companies to “[t]ap into unique engagement solutions and immersive formats to creatively and authentically connect without audiences around the world,”⁴⁸ consumer privacy experts have asserted legitimate concerns over TikTok’s connection to the Chinese government, and the possibility that TikTok’s robust collection of user information could be used without appropriate consent, and for improper purposes.⁴⁹

76. TikTok is a video streaming service that regularly delivers video content to users and maintains a cache of videos and virtual materials, including content from users, verified users, and advertisers.

77. TikTok’s terms state that it discloses users’ “video watches,” as well as usernames, device IDs and IP addresses, and other device activity.⁵⁰ In order to disclose this information, based upon information and belief, Plaintiffs believe that TikTok would also share the personalized profile of users that it uses to deliver highly-specific content to other users.⁵¹

78. TikTok does not provide distinct and separate disclosure regarding users’ video watches, nor does it require written consent distinct from other forms of consent or obligations either at the time TikTok sought to disclose users’ video viewing histories or in advance of sharing those viewing histories for a set duration of time.

⁴⁷ Mikey Dunn, *What You Need to Know About Advertising on TikTok*, Social Media Today (Aug. 20, 2019), <https://www.socialmediatoday.com/news/what-you-need-to-know-about-advertising-on-tiktok/561235/>.

⁴⁸ *TikTok Ads*, TikTok, <https://ads.tiktok.com/homepage/> (last accessed June 6, 2020).

⁴⁹ Justin Sherman, *Unpacking TikTok, Mobile Apps and National Security Risks*, Lawfare (Apr. 2, 2020), <https://www.lawfareblog.com/unpacking-tiktok-mobile-apps-and-national-security-risks>.

⁵⁰ *Privacy policy*, TikTok (Jan. 2020) <https://www.tiktok.com/legal/privacy-policy?lang=en>.

⁵¹ Jia Tolentino, *How TikTok Holds Our Attention*, New Yorker (Sept. 23, 2019), <https://www.newyorker.com/magazine/2019/09/30/how-tiktok-holds-our-attention>.

G. TikTok's Collection of Stored Communications and Messaging History

79. In addition to the privacy concerns raised by TikTok's other practices, the app regularly "collect[s] and process[es] [messages], which includes scanning and analyzing, information you provide, in the context of composing, sending, or receiving messages through our Service's messaging functionality," and that the information collected "includes the content of the message and information about when the message has been sent, received and/or read, as well as the participants of the communication."⁵²

80. Users' messages are transmitted from the users' mobile device to TikTok's servers, and from TikTok's servers to its affiliates' servers located abroad. TikTok allows users to send and receive messages, and it retains those messages in storage.

81. TikTok's terms state that it discloses this information to business partners and corporate affiliates.⁵³ With respect to TikTok's business partners, the terms state that TikTok will share users' information it collects (including messages) with business partners "to help perform business operations and for business purposes . . . including research, payment processing and transaction fulfillment, database maintenance, administering contests and special offers, technology services, deliveries, email deployment, advertising, analytics, measurement, data storage and hosting, disaster recovery, search engine optimization, marketing, and data processing."⁵⁴

82. In response to an inquiry about TikTok's data transfer to Chinese affiliates, TikTok spokesperson stated that as of February 2019 that TikTok user data is stored and processed in the U.S. and other markets where TikTok operates at industry-leading third-party data centers. The spokesperson went on to state that data still would be shared with others in their corporate group for the explained purposes, but never explained that purpose.

⁵² *Privacy policy*, TikTok (Jan. 2020) <https://www.tiktok.com/legal/privacy-policy?lang=en>.

⁵³ *Id.*

⁵⁴ *Id.*

83. There is also a close connection between ByteDance Ltd. of TikTok. Kevin Mayer, former Walt Disney Company streaming executive, will be the CEO of TikTok and COO of ByteDance Ltd.⁵⁵

84. ByteDance has goals of being an international player for quite some time. One former ByteDance manager who left in 2019 stated: “They want to be a global company, and numbers-wise, they’ve had that success. . . But the purse is still in China: The money always comes from there, and the decisions all come from there.”⁵⁶

85. TikTok’s sharing with corporate affiliates falls outside the scope of the above terms. The terms state that TikTok will share personal information (including messages) with its corporate affiliates to “improv[e] and optimis[e] the Platform, preventing illegal use and supporting users.”⁵⁷ Yet TikTok’s sharing with its corporate parent in China, as well as potentially the Chinese government, does not clearly fall under the scope of this provision since it does not clearly improve or optimize TikTok’s platform.⁵⁸

86. As such, neither Plaintiffs nor the class have provided the appropriate consent in order for TikTok to legally share this information.

H. Defendants Obscure The Terms of Use and Privacy Policy

87. TikTok also makes no effort to ensure users see the full text of the Terms of Use and Privacy Policy. When downloading the App, one step of the process invites users to “Text [themselves] a link to download TikTok.” This action is tied to the smallest text on the page though, which also places the small gray text on a black background, making the text less readable.⁵⁹

⁵⁵ Brooks Barnes and Jack Nicas, *Disney’s Head of Streaming Is New TikTok C.E.O.*, The New York Times (May 18, 2020), <https://www.nytimes.com/2020/05/18/business/media/tiktok-ceo-kevin-mayer.html?searchResultPosition=3>.

⁵⁶ Drew Harwell and Tony Romm, *Inside TikTok: A culture clash where U.S. views about censorship often were overridden by the Chinese bosses*, The Washington Post (Nov. 5, 2019), <https://www.washingtonpost.com/technology/2019/11/05/inside-tiktok-culture-clash-where-us-views-about-censorship-often-were-overridden-by-chinese-bosses/>.

⁵⁷ *Id.*

⁵⁸ Helen Ehrlich, *TikTok is Scamming People & Stealing Information*, Affinity Magazine (Nov. 4, 2018), <http://culture.affinitymagazine.us/tik-tok-is-scamming-people-stealing-information/>.

⁵⁹ Users are able to view videos without having to create an account. However, when they want to post content to the platform, they are required to go through a mandatory sign-in process where viewing the Terms of Service and Privacy Policy is not mandatory.

1 88. The text states, “By clicking the ‘send’ button, you confirm that you agree to our Terms of
2 Use and acknowledge you have read and understood our Privacy Policy.” But the Terms of Use and
3 Privacy Policy documents are not featured on the page nor is review presented as a mandatory step for
4 using the App.

5 89. TikTok intends this design to have the effect of a clickthrough legal agreement—in other
6 words, when users click the “send” button, TikTok considers this to be acceptance of a contract. But
7 TikTok has made a number of design decisions that increase the likelihood of the legal agreement not
8 being noticed by the end user. Specifically:

- 9 a. The text is the smallest text on the page. This reduces the legibility of the information and
10 makes it possible for users to simply not notice it;
- 11 b. The text is in low contrast. The text is gray (#DCDCDE), on a black (#000000) background,
12 making the contrast so low that it fails the WCAG 2.0 success criterion 1.4.6 pass indicator
13 for fonts below 18 points, making it likely that consumers will not be able to read or notice
14 the text;
- 15 c. The text is positioned below the “send” button—meaning that in certain situations, some
16 users may have their viewpoint arranged so that the legal agreement is hidden “below the
17 fold” (*i.e.*, off-screen), and they proceed to the next page never having read the text;
- 18 d. The Terms of Use and Privacy Policy documents are not presented as a mandatory step,
19 nor is the user required to select a checkbox or radio button to explicitly indicate that they
20 have read and understood them (meaning that a user can tap the “send” button without
21 noticing or reading the Terms of Use and Privacy Policy).

22 90. Importantly, a user can install the TikTok app and become a TikTok content customer
23 without proceeding through a clickthrough agreement containing the Terms of Use and Privacy Policy.
24 For example, the user may go directly to the Apple iOS App Store, download the App, and start using it
25 to look at videos. In that series of steps, the user is not shown any information about, nor links to the
26 Terms of Use or Privacy Policy.

91. TikTok’s designers have the ability to ensure that consumers read TikTok’s Terms of Service and Privacy Policy, but it has elected not to do so. For example, TikTok designers have required users to provide their birthday (meaning that 100% of users who complete the sign-up process must provide a date of birth, but not all users will have read the Terms of Use or Privacy Policy).

92. Requiring consumers to read and review terms of use with an explicit opt-in has been common practice in the design of end-user license agreements since the 1990s.

93. By making the Terms of Use and Privacy Policy difficult to read, and by not requiring consumers to read those documents, Defendants are able to hide terms that insulate them from lawsuits. TikTok requires users to arbitrate their disputes, complete with a ban on participation in class actions; however, few users would understand that they have consented to these terms—because they are not required to read them before using TikTok.

94. Given TikTok’s deliberate design choices to prevent consumers from receiving notice of what information is being disclosed, TikTok’s arbitration clause and class action ban is void and unenforceable.

I. TikTok’s Rise in Popularity During the Novel Coronavirus 2019 Pandemic

95. Official reports as of April 21, 2020 stated that TikTok has over 500 million monthly users, and has been downloaded over 1 billion times on the Google Play Store.⁶⁰ The application is being downloaded and used more now than ever before in its history, likely due to the severe acute respiratory syndrome coronavirus 2 (SARS-CoV-2 or “COVID-19”) pandemic and resulting quarantines. Many celebrities and internationally known athletes have downloaded the app and millions of others use the app as a means of staying entertained during these times.⁶¹

96. According to a recent article in Music Business Worldwide, the app was downloaded 2 million times in the week of March 16th—around the time of many shutdown and stay-at-home orders

⁶⁰ Tara Johnson, *The Rise of TikTok During COVID-19*, Tinuiti (Apr. 21, 2020), <https://tinuiti.com/blog/marketing-news-covid-19/tiktok-covid-19/>.

⁶¹ *Id.*

throughout the world.⁶² According to the report, this marked an 18% increase in downloads from the week before.⁶³ There was an increase of 27% to download rates throughout the first 23 days of March as well, again covering the span of the initial quarantine orders.⁶⁴ It has been so linked to the shutdowns that the hashtag #boredathome—tied to Curtis Roach’s song “Bored in the House”—was trending during the same time period, which was used where users were showing what they were doing just to pass the time, “while bored stuck in the house.”⁶⁵

97. The COVID-19 pandemic is impacting the nation’s political landscape as well, forcing many campaigns and officeholders to do more work online.⁶⁶

98. CNN Business emphasized the platform’s utility for millions of users in allowing them to bring out their creativity during quarantine.⁶⁷ PRNewswire developed an entire webinar in 2020 titled “TikTok: Best Practices & How to Make it Work for Your Brand During the COVID-19 Pandemic.”⁶⁸ Even therapists are utilizing the app in order to assist users in getting through quarantine and the pandemic.⁶⁹

⁶² Murray Stassen, *Coronavirus Quarantine Appears to be Driving a Global TikTok Download Boom*, Music Business Worldwide (Mar. 24, 2020), <https://www.musicbusinessworldwide.com/coronavirus-quarantine-appears-to-be-driving-a-global-tiktok-download-boom/>.

⁶³ *Id.*

⁶⁴ James Crowley, *TikTok Users Soar Now that Everybody Is at Home Trying to Get Famous*, Newsweek (Mar. 25, 2020), <https://www.newsweek.com/tiktok-users-soar-viral-videos-coronavirus-covid-19-1494229>, (“With people stuck at home self-isolating, TikTok has seen a spike in users and downloads as more people try to get their videos to go as viral as COVID-19. Sorry, the joke had to be made.”).

⁶⁵ *Id.*

⁶⁶ Samanta J. Gross, *As COVID-19 forces campaigns to go digital, Florida Democrats lag behind GOP*, Tampa Bay Times (May 24, 2020), <https://www.tampabay.com/news/health/2020/05/24/as-covid-19-forces-campaigns-to-go-digital-florida-democrats-lag-behind-gop/>; *TikTok becomes political platform ahead of US election*, Financial Times, <https://www.ft.com/content/c4c09793-993e-4ffd-9e46-2c609f98b79d>.

⁶⁷ *Quarantine bringing out creativity for millions on TikTok*, CNN Business, <https://edition.cnn.com/videos/media/2020/05/15/max-foster-tik-tok-during-lockdown-pkg-vpx.cnn>.

⁶⁸ Webinar: Best Practices & How to Make it Work for Your Brand During the COVID-19 Pandemic, <https://www.prnewsonline.com/webinars/tik-tok-best-practices-how-to-make-it-work-for-your-brand/>.

⁶⁹ Kaya Yurieff, *These therapists are using TikTok to help you get through the pandemic*, CNN Business (May 15, 2020), <https://www.cnn.com/2020/05/15/tech/tiktok-therapists/index.html>.

99. TikTok has seen a boom in users and downloads since the onset of this pandemic and continues to see the breadth of usership expand into all fields of professional life and all age ranges. The application has appealed to nearly everyone, with over 2 billion downloads to-date, and is one of the most utilized apps during quarantine by users of all backgrounds.

J. Fraudulent Concealment and Tolling

100. All applicable statutes of limitation have been tolled by Defendants' knowing and active fraudulent concealment and denial of the facts alleged herein through the time period relevant to this action.

101. Instead of disclosing Defendants' practice of collecting, storing, using and disclosing users' biometric identifiers and biometric information, as well as users' personally identifiable information and video viewing information, Defendants concealed this practice from users by not disclosing it to users or making this information otherwise available. Defendants concealed this information to encourage users to download and use the App.

102. Despite reasonable diligence on their part, Plaintiffs remained ignorant of the factual bases for their claims for relief. Defendants' withholding of material facts concealed the claims alleged herein and tolled all applicable statutes of limitation.

V. CLASS ACTION ALLEGATIONS

103. Plaintiffs bring this class action on behalf of themselves and other similarly situated individuals. Pursuant to Rules 23(a), (b)(1), (b)(2) and (b)(3) of the Federal Rules of Civil Procedure, Plaintiffs seek to certify a class of:

Nationwide Class: All persons residing in the United States who have used the Musical.ly and TikTok Apps on their mobile devices.

104. Plaintiffs also bring this class action on behalf of themselves and the following subclasses:

California Subclass: All Nationwide Class members who, while residing in California, used the Musical.ly and TikTok Apps on their mobile devices.

Illinois Subclass: All Nationwide Class members, who while residing in Illinois, used face filters, face stickers, or the face tracker lens on an image or video of their face or whose face appeared in a video uploaded to the Musical.ly or TikTok Apps while residing in Illinois.

105. Excluded from the Class and subclasses are Defendants, any entity in which any Defendant has a controlling interest, and its legal representatives, officers, directors, employees, assigns and successors. Also excluded from the Class is any judge, justice or judicial officer presiding over this matter and the members of their immediate families and judicial staff.

106. **Numerosity.** The number of members in the Class (and subclasses) is so numerous that joinder is impracticable. The precise number of class members can be determined through discovery, including discovery of Defendants' business records, by reference to objective criteria. At a minimum, the Class is made up of thousands of members.

107. **Common Questions of Law and Fact Predominate.** There are questions of law and fact common to Plaintiffs and class members, and those questions predominate over any questions that may affect any individual class member. Such common questions of law and fact include, but are not limited to:

- a. Whether Defendants' activities and practices referenced above and as alleged below constitute violations of the statutory causes of action alleged herein;
- b. Whether Defendants' activities and practices, if they did constitute violations of the statutory causes of action alleged herein, were willful;
- c. Whether Defendants' activities and practices referenced above constitute quantum meruit concerning which restitution and/or disgorgement is warranted;
- d. Whether Plaintiffs and members of the class sustained damages as a result of Defendants' activities and practices referenced above, and, if so, in what amount;
- e. Whether Defendants profited from their activities and practices referenced above, and, if so, in what amount; and
- f. Whether Plaintiffs and class members are entitled to declaratory and injunctive relief.

108. **Typicality.** Plaintiffs' claims are typical of the claims of all members of the Class and subclasses. Their claims arise from the same practices and conduct that give rise to the claims of all class members and are based on the same legal theories.

1 109. **Adequacy.** Plaintiffs will fairly and adequately protect the interests of the Class. They have
2 no interests antagonistic to those of the other class members and are committed to vigorously prosecuting
3 this case. Plaintiffs have retained counsel experienced in consumer class actions and complex litigation
4 involving privacy and data security.

5 110. **Superiority.** A class action is superior to other available methods for the fair and efficient
6 adjudication of this controversy. Given that the relative amount of each Class member's is small relative
7 to the expense of litigating those claims, and given Defendants' financial resources, no Class member is
8 likely seek legal redress on an individual basis for the violations alleged in this complaint. Individual
9 actions would significantly increase the expense to all parties, burden the court with duplicative litigation,
10 and create a risk of inconsistent or varying adjudications that would establish incompatible standards of
11 conduct for Defendants. Separate actions by individual class members would also risk adjudications that
12 would, as a practical matter, be dispositive of the interests of the other members not parties to the
13 individual adjudications or would substantially impair or impede their ability to protect their interests. A
14 class action, however, promotes an orderly and expeditious adjudication of the Class claims, presents
15 fewer management difficulties, and ensures comprehensive supervision in a single forum.

16 111. **Injunctive Relief Appropriate.** Defendants acted and refused to act on grounds generally
17 applicable to the Class, thereby making appropriate final injunctive relief with respect to the members of
18 the Class as a whole.
19
20
21
22
23
24
25
26
27
28

VI. CAUSES OF ACTION

NATIONWIDE CAUSES OF ACTION

COUNT I

VIOLATION OF THE COMPUTER FRAUD AND ABUSE ACT

18 U.S.C. §§ 1030, *et seq.*

(On Behalf of Plaintiffs, the Nationwide Class, and, in the alternative, Subclasses)

112. Plaintiffs incorporate the foregoing allegations in paragraphs 1 through 111 as if fully set forth herein.

113. The mobile devices belonging to Plaintiffs and class members are “protected computers” within the meaning of 18 U.S.C. § 1030(e)(2)(B) in that they are “used in or affecting interstate or foreign commerce or communication[.]”

114. Defendants caused Plaintiffs and class members to download and install the App to their mobile devices without informing users that the App contained code that went beyond what users expected the App to do, the information that was collected by the App, and the information that was disclosed by the App.

115. By surreptitiously collecting, storing, and using Plaintiffs’ and class members’ personally identifiable information without prior disclosure and consent, Defendant knowingly exceeded its authorized access to Plaintiffs’ and class members’ protected computers, in violation of 18 U.S.C. § 1030(a)(2)(C).

116. Defendants’ actions caused injuries to users as set forth herein because of the numerous threats to public safety caused by Defendants’ surreptitious violations of user privacy, and failure to obtain consent before collecting and disclosing certain user information.

117. Plaintiffs, on behalf of themselves and class members, accordingly seek compensatory damages, injunctive relief, and other equitable relief as allowed by 18 U.S.C. § 1030(g).

COUNT II
VIOLATION OF THE VIDEO PRIVACY PROTECTION ACT
18 U.S.C. § 2710, et seq.

(On Behalf of Plaintiffs, the Nationwide Class, and, in the alternative, Subclasses)

118. Plaintiffs incorporate the foregoing allegations in paragraphs 1 through 111 as if fully set forth herein.

119. Plaintiffs reallege and incorporate by reference every allegation set forth in the preceding paragraphs as though alleged fully herein.

120. The VPPA provides that “a video tape service provider who knowingly discloses, to any person, personally identifiable information concerning any consumer shall be liable to the aggrieved person for the relief provided in subsection (d).” 18 U.S.C. § 2710(b)(1). Defendant TikTok violated this statute by knowingly disclosing personally identifiable information to ByteDance Ltd. and other corporate affiliates.

121. Defendant TikTok is a “video tape service provider” under 18 U.S.C. § 2710(a)(4) because it “engaged in the business, in or affecting interstate or foreign commerce, of rental, sale, or delivery of prerecorded video cassette tapes or similar audio-visual materials.” TikTok is engaged in the business of delivering video content and services to its users, including Plaintiffs. TikTok’s platform allows users to create, post, share, view, and otherwise engage with videos. TikTok platform is built to deliver video content to consumers. TikTok regularly delivered videos to TikTok’s subscribers, including Plaintiffs, by making those materials electronically available to Plaintiffs on TikTok’s platform. TikTok also allowed users to create, and share videos with a non-public audience.

122. Plaintiffs and class members are “consumers” under 18 U.S.C. § 2710(a)(1) because they are “subscriber[s] of goods or services” from TikTok. Plaintiffs and class members are registered TikTok users who use the website and mobile application through interaction with it. Plaintiffs and class members were required to provide personally identifiable information to TikTok, including date of birth, in order to sign up, become registered users, establish user profiles, to subscribe to “follow” other accounts, and to contribute to TikTok’s video streaming content. By signing up for accounts with TikTok, becoming registered users, establishing user profiles, providing TikTok with personal information, and spending time and attention using and contributing to TikTok’s video streaming platform, Plaintiffs and class

1 members entered into transactions with TikTok to obtain access to TikTok's content and services and for
2 the purpose of subscribing to TikTok's video streaming content and services.

3 123. The VPPA defines "personally identifiable information" to "include[] information which
4 identifies a person as having requested or obtained specific video materials or services from a video tape
5 service provider." 18 U.S.C. § 2710(a)(1)(3). TikTok "knowingly disclose[d]" to corporate affiliates
6 users' personally identifiable information, including what videos a user has watched; whether a user has
7 engaged with videos by downloading, liking, commenting and/or sharing the video; how long the user
8 views the video; whether the user saves the video to their "Favorites" page; and accounts the user follows.
9 TikTok's disclosure also included personally identifiable information because the information shared
10 included a user's: username, device information, and location data.

11 124. Defendant TikTok disclosed personally identifiable information to corporate affiliate,
12 ByteDance Ltd., through the transfer to at least three domains: maliva-mcs.byteoversea.com, sgali-
13 mcs.byteoversea.com, and mon-va.byteoversea.com. Upon information and belief, these domains are
14 owned and operated by ByteDance Ltd.

15 125. Every time a user visits the platform, TikTok transfers to ByteDance Ltd., through the
16 domain of either mon-va.byteoversea.com or sgali-mcs.byteoversea.com: the URL of the video watched;
17 the duration that the user watched the video for; and the time the user watched it. TikTok also sends to
18 ByteDance: the user's UID, unique UID, SSID, and web_ID.

19 126. TikTok transfers to ByteDance, through the domain mon-va.byteoversea.com domain: the
20 specific URL of the video watched by the user and the unique identifier titled SLARDAR_WEB_ID.

21 127. TikTok maintains the same UID for each individual user. While a user is logged on to the
22 platform, TikTok pairs the same UID with the video viewing information it transmits to ByteDance Ltd.
23 This UID follows the user every time she logs on to the platform regardless of the device, and even after
24 she may have cleared her browser history and cookies. The additional Unique Identifiers that TikTok
25 transmits to ByteDance, allow ByteDance to continue identifying users' viewing activity even when they
26 are not logged on but are still viewing videos on the platform. When the user visits her profile page, these
27 Unique Identifiers are easily linked to the user's account name, and profile page. The profile page contains
28

1 information that can further identify individuals by name since it includes an uploaded biography and
2 videos that the user has shared.

3 128. TikTok's pairing of personal information, including user's account name and Unique
4 Identifiers, with users' video viewing history violates the VPPA because it readily shows which requested
5 or obtained specific video materials.

6 129. TikTok did not inform users of its pattern and practice of disclosing personally identifiable
7 information and does not obtain their consent to such disclosure.

8 130. Unlawful disclosure of personally identifiable information concerning Plaintiffs and class
9 members was not incident to the "ordinary course of business" of delivering the visual content as that term
10 is defined by the VPPA. *See* 18 U.S.C. § 2710(a)(2). The disclosure of users' personally identifiable
11 information to third parties not involved in the transactions as alleged herein was not necessary in order
12 for TikTok to deliver those prerecorded visual materials to Plaintiffs and class members.

13 131. The VPPA also provides that a video tape service provider may nonetheless disclose
14 personally identifiable information concerning a consumer as long as that person has provided "informed
15 written consent . . . in a form distinct and separate from any form setting forth other legal or financial
16 obligations of the consumer." 18 U.S.C. § 2710(b)(2)(A)(i).

17 132. However, TikTok failed to obtain the "informed, written consent" of Plaintiffs and class
18 members "in a form distinct and separate from any form setting forth other legal or financial obligations
19 of the consumer" and "at the election of the consumer," either "given at the time the disclosure is sought"
20 or "given in advance for a set period of time, not to exceed 2 years or until consent is withdrawn by the
21 consumer, whichever is soon." *See* 18 U.S.C. § 2710(b)(2)(B)(i)-(ii). No TikTok document complied with
22 these requirements.

23 133. The VPPA also requires that "[a] person subject to the section shall destroy personally
24 identifiable information as soon as practicable, but no later than one year from the date the information is
25 no longer necessary for the purposes for which it was collected" 18 U.S.C. § 2710(e). Upon
26 information and belief, TikTok does not destroy this information and maintains users' personally
27
28

1 identifiable information despite the fact that it is no longer necessary for purposes of delivering the
2 prerecorded visual information, in violation of the VPPA.

3 134. On behalf of themselves and other class members, Plaintiffs seek to recover awarded actual
4 damages, not less than liquidated damages in the amount of \$2,500 per Plaintiff, punitive damages,
5 attorneys' fees and costs, and such other preliminary and equitable relief as the Court determines to be
6 appropriate. 18 U.S.C. § 2710(c)(2).

7 **COUNT III**
8 **QUANTUM MERUIT TO RECOVER SUMS HAD BY UNJUST ENRICHMENT**
9 **(On Behalf of Plaintiffs, the Nationwide Class, and, in the alternative, Subclasses)**

10 135. Plaintiffs incorporate the foregoing allegations in paragraphs 1 through 111 as if fully set
11 forth herein.

12 136. Plaintiffs bring this count to pursue restitution based on Defendants' unjust enrichment,
13 including by way of Defendants' retention of profits that should have been expended to protect Plaintiff's
14 data as required by law.

15 137. Defendants have unjustly received and retained monetary benefit from Plaintiffs and class
16 members—*i.e.*, by way of their use of, and profiting from, their data under unjust circumstances, such that
17 inequity has resulted.

18 138. By engaging in the conduct described in this complaint, Defendants knowingly obtained
19 benefits from Plaintiffs and class members as alleged herein under circumstances such that it would be
20 inequitable and unjust for Defendants to retain them.

21 139. Defendants will be unjustly enriched if permitted to retain the benefits derived from
22 unlawful gathering and sharing of Plaintiff's and class members' data.

23 140. Plaintiffs are therefore entitled to restitution in an amount to be determined at trial, or the
24 imposition of a constructive trust upon the monies derived by Defendants by means of the above-described
25 actions, or as the circumstances may merit to provide complete relief to Plaintiffs.
26
27
28

STATE SUBCLASS CAUSES OF ACTION

COUNT IV
VIOLATION OF THE ILLINOIS BIOMETRIC PRIVACY ACT
FAILURE TO OBTAIN INFORMED, WRITTEN CONSENT
740 ILCS 14/15(b)
(On Behalf of Plaintiff Johnson and the Illinois Subclass)

141. Plaintiff Johnson incorporates the foregoing allegations in paragraphs 1 through 111 as if fully set forth herein.

142. The BIPA makes it unlawful for any private entity to “collect, capture, purchase, receive through trade, or otherwise obtain a person’s or a customer’s biometric identifier or biometric information unless it first: (1) informs the subject or the subject’s legally authorized representative in writing that a biometric identifier or biometric information is being collected or stored; (2) informs the subject or the subject’s legally authorized representative in writing of the specific purpose and length of term for which a biometric identifier or biometric information is being collected, stored, and used; and (3) receives a written release executed by the subject of the biometric identifier or biometric information or the subject’s legally authorized representative.” 740 ILCS 14/15(b).

143. TikTok is a California corporation and thus, qualifies as a “private entity” under the BIPA. 740 ILCS 14/10. ByteDance, Inc. is a Delaware corporation, with its principal place of business in California and thus, also qualifies as “private entity” under the BIPA. *Id.*

144. Plaintiffs and class members had their biometric identifiers or biometric information captured, collected, stored, and used by Defendants through the TikTok App. Defendants’ practice of collecting, storing and using Plaintiffs’ and class members’ biometric identifiers or biometric information violated Plaintiffs’ and class members’ right to privacy in their biometric identifiers or biometric information under the BIPA, 740 ILCS 14/1, *et seq.*

145. Defendant did not inform Plaintiffs and class members in writing that their biometric identifiers or biometric information would be “collected or stored” as required under 740 ILCS 14/15(b)(1).

1 146. Nor did Defendants inform Plaintiffs and class members in writing of the “specific purpose
2 and length of term for which [their] biometric identifier or biometric information is being collected, stored,
3 and used” as required under 740 ILCS 14/15(b)(2).

4 147. Defendants also did not receive “a written release executed by the subject of the biometric
5 identifier or biometric information or the subject’s legally authorized representative.” 740 ILCS
6 14/15(b)(3).

7 148. Defendants acted intentionally or recklessly in collecting, storing and using Plaintiffs’ and
8 class members’ biometric identifiers or biometric information. As set forth herein, Defendants designed
9 the TikTok application to capture and collect biometric information of a user before the user even posts a
10 video. In the alternative, Defendants acted negligently when it collected, stored, and used Plaintiffs’ and
11 class members’ biometric identifiers or biometric without informing them in writing that this information
12 would be collected and without obtaining written consent.

13 149. TikTok purposefully avoided providing notices or obtaining consent from class members
14 in order to ensure that as many users downloaded and used the App as possible.

15 150. As a result of Defendants’ intentional and/or reckless violation of BIPA, Plaintiff Johnson
16 and Illinois Subclass Members already have been injured and will continue to be injured, in an amount to
17 be proven at trial.

18 151. On behalf of themselves and Illinois Subclass Members, Plaintiff Johnson seeks:
19 (1) injunctive and equitable relief as is necessary to protect the interests of Plaintiffs and Illinois Subclass
20 members by requiring TikTok to comply with the 740 ILCS 14/15(b) requirements for the collection,
21 storage, and use of biometric identifiers or biometric information and (2) statutory damages of \$5,000 per
22 intentional or reckless violation of BIPA pursuant to 740 ILCS 14/20(2) and statutory damages of \$1,000
23 per negligent violation of the BIPA pursuant to 740 ILCS 14/20(1); and (3) reasonable attorneys’ fees and
24 costs and other litigation expenses pursuant to 740 ILCS 14/20(3).

COUNT V
VIOLATION OF THE ILLINOIS BIOMETRIC PRIVACY ACT
FAILURE TO INSTITUTE AND MAINTAIN PUBLICLY-AVAILABLE
RETENTION SCHEDULE
VIOLATION OF 740 ILCS 14/15(a)
(On Behalf of Plaintiff Johnson and the Illinois Subclass)

152. Plaintiff Johnson incorporates the foregoing allegations in paragraphs 1 through 111 as if fully set forth herein.

153. The BIPA makes it unlawful for any private entity to “collect, capture, purchase, receive through trade, or otherwise obtain a person’s or a customer’s biometric identifier or biometric information unless it first: (1) informs the subject or the subject’s legally authorized representative in writing that a biometric identifier or biometric information is being collected or stored; (2) informs the subject or the subject’s legally authorized representative in writing of the specific purpose and length of term for which a biometric identifier or biometric information is being collected, stored, and used; and (3) receives a written release executed by the subject of the biometric identifier or biometric information or the subject’s legally authorized representative.” 740 ILCS 14/15(b).

154. Plaintiff Johnson and Illinois Subclass Members had their biometric identifiers or biometric information captured, collected, stored, and used by Defendants through the TikTok App.

155. TikTok is a California corporation and thus, qualifies as a “private entity” under the BIPA. 740 ILCS 14/10. ByteDance, Inc. is a Delaware corporation, with its principal place of business in California and thus, also qualifies as “private entity” under the BIPA. *Id.*

156. Defendants’ practice of collecting, storing and using Plaintiffs’ and Illinois Subclass members’ biometric identifiers or biometric information violated Plaintiffs’ and Illinois Subclass members’ right to privacy in their biometric identifiers or biometric information under the BIPA, 740 ILCS 14/1, *et seq.*

157. Defendants did not make available to the public, a written policy “establishing a retention schedule and guidelines for permanently destroying biometric identifiers or biometric information when the initial purpose for collecting or obtaining such identifiers or information has been satisfied or within

3 years of the individual's last interaction with the private entity, whichever occurs first” as required under 740 ILCS 14/15(a).

158. Defendants acted intentionally or recklessly in not making publicly available a data retention policy and guidelines for permanently destroying such identifiers or information, as required by 740 ILCS 14/15(a). Defendants did so to ensure that as many users downloaded and used the app as possible. As set forth herein, Defendants designed the TikTok application to capture and collect biometric information and biometric identifiers of users whenever they access the app and before they even posts videos. Defendants maintain users’ biometric information and biometric identifiers for an undisclosed period of time that exceeds the initial purpose for collecting or obtaining such identifiers or information.

159. In the alternative, Defendants acted negligently when they collected, stored, and used Plaintiff’s and Illinois Subclass members’ biometric identifiers or biometric information without making publicly available a data retention policy and guidelines for permanently destroying such identifiers or information, as required under 740 ILCS 14/15(a).

160. On behalf of herself and Illinois Subclass members, Plaintiff Johnson seeks: (1) injunctive and equitable relief as is necessary to protect the interests of Plaintiff and Illinois Subclass Members by requiring TikTok to make publicly available a policy for the permanent destruction of biometric identifiers or biometric information pursuant to 740 ILCS 14/15(a); (2) statutory damages of \$5,000 per intentional or reckless violation of BIPA pursuant to 740 ILCS 14/20(2) and statutory damages of \$1,000 per negligent violation of the BIPA pursuant to 740 ILCS 14/20(1); and (3) reasonable attorneys’ fees and costs and other litigation expenses pursuant to 740 ILCS 14/20(3).

COUNT VI
VIOLATION OF THE ILLINOIS BIOMETRIC PRIVACY ACT
DISCLOSURE OF BIOMETRIC IDENTIFIERS AND INFORMATION WITHOUT CONSENT
VIOLATION OF 740 ILCS 14/15(d)
(On Behalf of Plaintiff Johnson and the Illinois Subclass)

161. Plaintiff Johnson incorporates the foregoing allegations in paragraphs 1 through 111 as if fully set forth herein.

1 162. TikTok is a California corporation and thus, qualifies as a “private entity” under the BIPA.
2 740 ILCS 14/10. ByteDance, Inc. is a Delaware corporation, with its principal place of business in
3 California and thus, also qualifies as “private entity” under the BIPA. *Id.*

4 163. Plaintiff Johnson and Illinois Subclass Members had their biometric identifiers or biometric
5 information captured, collected, stored, and used by Defendants through the TikTok App. Defendants’
6 practice of disclosing, redisclosing, or otherwise disseminating Plaintiffs’ and Illinois Subclass members’
7 biometric identifiers or biometric information to undisclosed third parties and corporate affiliates violated
8 Plaintiffs’ and class members’ right to privacy in their biometric identifiers or biometric information under
9 the BIPA, 740 ILCS 14/1, *et seq.*

10 164. Defendants systematically and automatically “disclose[d], redisclose[d], or otherwise
11 disseminate” Plaintiff’s and the Class’s biometric identifiers and/or biometric information without first
12 obtaining the consent required by 740 ILCS 14/15(d)(1). Defendants disclosure or redisclosure was not
13 made as part of a “financial transaction requested or authorized” by Plaintiffs or class members, the
14 disclosure or redisclosure was not “required by State or federal law or municipal ordinance,” and the
15 disclosure was not required pursuant to a valid warrant or subpoena. 740 ILCS 14/15(d)(2)-(4).

16 165. Defendants acted intentionally or recklessly in disclosing, redisclosing, or otherwise
17 disseminating Plaintiff Johnson’s and Illinois Subclass members’ biometric identifiers or biometric
18 information. As set forth herein, Defendants designed the TikTok application to capture and collect
19 biometric identifiers and biometric information of a user before the user even posts the video. TikTok
20 purposefully avoided providing notices or obtaining consent from Plaintiff Johnson and the Illinois
21 Subclass members in order to ensure that as many users downloaded and used the App as possible.
22 Similarly, Defendants did not inform Plaintiff Johnson and Illinois Subclass members that their biometric
23 identifiers and biometric information was being distributed and/or redistributed to undisclosed corporate
24 affiliates, third parties, and other business partners.

25 166. In the alternative, Defendants acted negligently in disclosing, redisclosing, or otherwise
26 disseminating Plaintiff Johnson’s and Illinois Subclass members’ biometric identifiers or biometric
27 without obtaining written consent.
28

COUNT VII
VIOLATION OF THE CALIFORNIA PENAL CODE
Cal. Pen. Code § 484, 496
(On Behalf of Plaintiff Iyer and the California Subclass)

170. Section 496(a) prohibits obtaining property “in any manner constituting theft.”

Every person who shall feloniously steal, take, carry, lead, or drive away the personal property of another, or who shall fraudulently appropriate property which has been entrusted to him or her, or who shall knowingly and designedly, by any false or fraudulent representation or pretense, defraud any other person of money, labor or real or personal property, or who causes or procures others to report falsely of his or her wealth or mercantile character and by thus imposing upon any person, obtains credit and thereby fraudulently gets or obtains possession of money, or property or obtains the labor or service of another, is guilty of theft.

53. Defendant intentionally designed a program that deceived Plaintiff Iyer and California Subclass members into providing personally identifiable information to Defendant, including username, device information, and location data as well as video viewing history and interactions with video content,

1 such as whether a user has downloaded, liked, commented, shared the video, or added it to a “Favorites”
2 page.

3 54. Defendant acted in a manner constituting theft and/or false pretense by stealing, taking,
4 and/or fraudulently appropriating Plaintiff Iyer’s personally identifiable information without consent.

5 55. Defendant concealed, aided in concealing, sold, and/or used Plaintiff Iyer’s and California
6 Subclass members’ personally identifiable information for Defendant’s own commercial purposes and
7 financial benefit, including by sharing this information with third parties.

8 56. The reasonable and fair market value of the unlawfully obtained personal data can be
9 determined in the marketplace.

10 **PRAYER FOR RELIEF**

11 WHEREFORE, Plaintiffs, and each Class member, pray for judgment against Defendants as follows:

12 A. That this action and the proposed class be certified and maintained as a class action,
13 appointing Plaintiffs as representatives of the Class, and appointing the attorneys and law firms
14 representing Plaintiffs as counsel for the Class;

15 B. Enter Judgment against Defendants on Plaintiffs’ and class members’ asserted causes of
16 action;

17 C. For statutory damages of \$5,000 for each intentional or reckless violation of the BIPA, or
18 in the alternative, for statutory damages of \$1,000 for each negligent violation of the BIPA;

19 D. For statutory damages not less than \$2,500 per Plaintiff for violation of the VPPA;

20 E. For damages suffered as a result of the conduct alleged, punitive damages, restitution, and
21 disgorgement, to include interest and prejudgment interest;

22 F. For equitable, injunctive, and declaratory relief as may be appropriate;

23 G. For attorneys’ fees and costs as permitted by law;

24 H. For pre-judgment and post-judgment interest, as prescribed by law; and

25 I. For such additional legal and equitable relief as this Court may deem just and proper.
26
27
28

DEMAND FOR JURY TRIAL

Pursuant to Federal Rule of Civil Procedure 38(b), Plaintiffs demand a trial by jury on all causes of action so triable.

Dated: June 9, 2020

BLEICHMAR FONTI & AULD LLP

By: /s/ Lesley E. Weaver

Lesley E. Weaver (SBN 191305)
555 12th Street, Suite 1600
Oakland, CA 94607
Telephone: (415) 445-4003
Facsimile: (415) 445-4020
lweaver@bfalaw.com

DICELLO LEVITT & GUTZLER LLC

Amy E. Keller, *pro hac vice to be filed*
Ten North Dearborn Street
Sixth Floor
Chicago, IL 60602
Telephone: (312) 214-7900
Facsimile: (440) 953-9138
akeller@dicellolevitt.com

Counsel for Plaintiffs and the Putative Classes